

BEST AVAILABLE COPY

PCT/SE 03 / 0 1 8 8 2

PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

**Intyg
Certificate**

REC'D 19 DEC 2003

WIPO

PCT



Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71) Sökande Telefonaktiebolaget L M Ericsson (publ), Stockholm
Applicant (s) SE

(21) Patentansökningsnummer 0301964-3
Patent application number

(86) Ingivningsdatum 2003-07-03
Date of filing

Stockholm, 2003-12-09

För Patent- och registreringsverket
For the Patent- and Registration Office

Sonia André
Sonia André

Avgift
Fee

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

WLAN session control

Field of the invention

- 5 The invention relates to the field of providing session control in WLAN based networks. More particularly the invention relates to a method for session control in RADIUS-based networks. The invention may advantageously be utilised for providing timely user information in pre-paid WLAN solutions.

10

Prior art

- Wireless LAN (WLAN), and in particular WLAN based on the IEEE 802.11 standard, has in the last few years received tremendous interest. WLANs are used in home and enterprises environments. WLANs have also become available to WLAN subscribers at public sites, so called hot-spots, e.g. cafes, airports etc. In order to finance these hot spots, the owner of the WLAN infrastructure, such as the service provider, must be able to control access to the WLAN in order to charge customers for its use.

- 20 A hot spot typically has a number of Access Points (AP) and one or more access servers, here called Wireless Serving Node (WSN) and an authentication server (AS) as illustrated in fig. 1. The functionality of the WSN could also be integrated with each AP. The AS does not have to reside at the hot spot network but could be centrally located by the service provider or somewhere in the Internet.

25

- The most common solution today is that the access control and the collecting of accounting data are performed by the WSN. This solution has been schematically illustrated in fig. 2. The APs are simply pass-through devices when it comes to access control. Users log in to the system using a HTTP (Hypertext Transfer Protocol) web interface between the UE (User equipment) and WSN. The HTTP traffic between UE and WSN is typically cryptographically protected by e.g. SSL (Secure Socket Layer). In order to verify the credentials received from the UE, the WSN (Wireless Serving Node) typically has a RADIUS client that communicates with an Authentication Server (AS).

- 35 In fig. 4, the exemplary process of a user first connecting to a hot spot access point arrangement of fig. 2 and subsequently running out of credit is shown, whereby the authorisation is facilitated by means of "web login" (HTTP).

These steps shall be briefly described here. In steps 21-27 the well-known steps of the station STA1 authenticating itself and subsequently being accepted for association by the access point AP1 is shown. In step 50 the user of the station opens a web browser and forwards a HTTP Get request 53. The requested web address (URL) does not have to point to the gateway node WSN since the WSN can intercept and redirect the request. The gateway node responds by issuing a HTTP log in page 55. The user then enters his name and password 57 and forwards this information to the gateway node WSN. Upon acceptance the gateway provides a HTTP session window 61, issues a start accounting message to the authentication server AS 63 and opens for traffic to/from the station 65.

At some later stage the user may run out of credit. This could be detected in different ways. The gateway can e.g. periodically report to the authentication server, which detects that the account is null 53. Alternatively, the AS, or some other network node, could have a timer to detect when the session should end. The authentication server issues a lock out request 69, whereupon the gateway node locks out the station 71.

Recently, a new method, denoted IEEE 802.1X, for performing access control at an extended level of security has been introduced under the IEEE 802.11i standardization task group and elsewhere. According to this method, schematically illustrated in fig. 3, access control is performed in the AP. For this purpose, the AP typically has a RADIUS client that talks to the AS. The UE and AS communicate using the Extensible Authentication Protocol (EAP). The WSN may still be used to provide various kinds of services, e.g. collecting accounting data, enforcing user profiles etc.

When the UE moves it may leave radio coverage of one AP (the "previous" AP) and move into coverage of another AP (the "subsequent" AP). In this case the UE has to make a handover from the previous AP to the subsequent AP. The IEEE 802.11 standard provides a method for making this handover. In particular, there is support for the 802.11-defined Association with the subsequent AP but there is no way to tell the previous AP that the UE has moved to another AP. The previous AP has to discover by implicit means, e.g. based on timeouts, that the UE is no longer in its cell.

To remedy this problem a new recommended practice has been approved according to 802.11F that specifies an Inter-AP Protocol (IAPP). The purpose of this protocol is to introduce a standardized way for APs to communicate when an UE associates or makes

a handover. According to the IAPP, the "subsequent" AP can send an IAPP message to the "previous" AP and let it know that the UE is now associated with the "subsequent" AP. The "previous" AP can then remove the UE from its memory. The "previous" AP shall at that point also send an 802.11 Disassociation message to the UE according to 802.11F. Moreover, the IAPP facilitates transfer of cryptographically protected information between the APs.

In fig. 5, an exemplary handshake diagram illustrates the process of a user approaching and connecting to a hot spot access point and subsequently moving to another AP within the hot spot network being configured as in fig. 1 using RADIUS and 802.1X authentication and 802.11F.

The legacy 802.11 steps of authentication and association are performed in steps 21- 27 after the Station STA1 comes within reach of the AP1. Subsequently, an 802.1X authentication procedure before the authentication server AS is initiated. The AP issues a request ID 29 and the station responds 31. The access point AP1 sends a RADIUS access request 33 to the authentication server AS with information about the user identity. Then follows an EAP message exchange 35 to perform the authentication. The details of this exchange depend on which authentication method is used. Here EAP is chosen by way of example. If the authentication is successful, the AS sends a RADIUS access accept 37 and the AP transmits a success 39 to the station, while the AP opens for traffic 40 for the station in question. The gateway node WSN initiates charging of the traffic running through it relating to the station.

Should the station move into the approach of AP2, 802.11 legacy steps of re-authentication and re-association is performed in steps 43 – 46. According to the IAPP protocol, AP2 issues the IAPP move message 47 to AP1, which responds with an IAPP move confirm message 49, which may include a context including e.g. the credentials relating to the authentication between the station STA1 and the authentication server AS. Finally, AP1 may issue a Disassociate message 51 to AP1 according to 802.11F, which is now informed that it can cancel information relating to STA1.

Some AP vendors have implemented a IAPP related (non-standardized) functionality: If a layer-2 frame appears on the wired network side of the (previous) AP with the UE's MAC address as the source address, the AP knows that the UE must be associated to

some other (subsequent) AP. The previous AP can then remove the UE from its memory and transmit a Disassociation message to the UE.

5 In many cases it may be desirable to close an ongoing session from the WSN or some other node that is not the AP, e.g. if the user has a pre-paid account that runs out of credit. Another scenario is that the user has been idle for a long time, e.g. if he/she has left the laptop at the hot spot unattended. In this case the WSN may want to force the UE to perform a re-authentication. The WSN can easily close an active session and/or force a re-authentication if access-control is performed in WSN, e.g. if web-login is used.

10 If the system is running 802.1X the situation is different. In this case access control is performed in the APs and there is no standardized way for the WSN to tell the APs to close an active session or to force a re-authentication. In particular, RADIUS has no server-initiated messages that can be used by the WSN or other entity to e.g. close the session or to initiate a new authentication.

15 The solution where the WSN just blocks all traffic to/from the user is not useful since the user will not be able to discover why he/she has no access to the internet. In a scenario without the WSN it is not even possible to block the traffic from the UE in question.

20 One possible solution is that the WSN waits for the next re-authentication. Subsequently, the AS may reject this re-authentication attempt. Moreover, since the RADIUS messages from the RADIUS client in the AP will pass the WSN, the WSN can make sure that the authentication is rejected. In any case the session will end. The drawback with this solution is that the time between re-authentications can be long (default 802.1X re-authentication interval is one hour). The WSN will thus have a very weak control of the session.

30 Another possibility is to implement a proprietary protocol between AP and WSN for session control. The drawback with this solution is that only APs of a certain type can be used together with the WSN.

35 A third possibility is to use DIAMETER instead of RADIUS as the authentication protocol since DIAMETER has server-initiated messages that can be used to close a session. However, RADIUS is the single preferred solution by vendors today and the author of this invention knows of no APs with DIAMETER support.

Summary of the invention

It is a first object of the invention to set forth a network for a controlling a station to terminate its access to a given AP.

5

This object has been accomplished by the subject matter set forth in claim 1.

It is a further object to set forth an access control node, for a controlling a station to terminate its access to a given AP.

10

This object has been accomplished by the subject matter of claim 7.

It is a further object to set forth a method, for a controlling a station to terminate its access to a given AP.

15

This object has been accomplished by the subject matter of claim 9.

Further advantages will appear from the detailed description of the invention.

20

Brief description of the drawings

Fig. 1 shows a hot spot network having a number of Access Points (AP) and one or more access servers, here called WLAN Serving Node (WSN) and an access server (AS),

25

fig. 2 shows a prior art network where access control and collection of accounting data is performed by a gateway node (WSN),

30

fig. 3 shows a prior art method, denoted IEEE 802.1X, for performing access control at an extended level of security under e.g. the IEEE 802.11i standardization task group and Wi-Fi Protected Access.

- fig. 4 shows an exemplary prior art process of a user first connecting to a hot spot access point arrangement of fig. 2 and subsequently running out of credit is shown, whereby the authorisation is facilitated by means of "web login" (HTTP),
- 5 fig. 5 is an exemplary prior art handshake diagram illustrating the process of a user approaching and connecting to a hot spot access point and subsequently moving to another AP within the hot spot network being configured as in fig. 1 using RADIUS and 802.1X authentication and IAPP,
- 10 fig. 6 is a handshake diagram of a first embodiment according to the invention having a network topology resembling the prior art network shown in fig. 1,
- fig. 7 is a handshake diagram of a second embodiment according to the invention
- 15 fig. 8 is a handshake diagram of a third embodiment according to the invention
- fig. 9 is a handshake diagram of a fourth embodiment according to the invention, and
- fig. 10 is a handshake diagram relating to denial of service attack in relation to the invention.
- 20

Detailed description of preferred embodiments of the invention

25

According to the invention the WSN or another non-AP network node uses the IAPP protocol and/or the layer-2 frames to cancel a session in one or several APs. According to the invention the termination could typically be used in connection with an accounting system, whereby the access termination is caused by the exhaustion of a given account of a using entity. It is a prerequisite for the invention that the AP supports the IAPP functionality described above in relation to the prior art. Hence, the invention could appropriately be used in a scenario where an agreement has been made between the AP's in question, the WSN and the AS. One party could also own these entities.

35

In fig. 6 a first embodiment according to the invention has been shown. The architecture of the network could advantageously resemble the prior art network shown in fig. 1, whereby a station STA is connected to AP's AP1 or AP2 of the same network segment but where the node WSN does not necessarily function as a gateway, i.e. constitute the only route to the Internet. Rather, the function of the WSN node will be elucidated in the following description.

In step 101, the account relating to the station STA is exhausted and the AS transmits a Lock out Request 103 to the WSN node in order to notify the WSN that the user in question should cease to have access to the Internet. If the WSN has a gateway position, i.e. it constitutes the only route to the Internet for AP1 and AP2, the WSN node could block traffic relating to STA1. This option has been shown by the lock out action 105.

Subsequently, the WSN issues an IAPP move notify to the AP's AP1 and/or AP 2 as indicated by steps 107 and 111. If the WSN knows to which AP the STA1 is associated, it may be enough to issue an IAPP move notify to that AP. It is noted that the WSN not necessarily being an AP is emulating an AP by issuing AP specific messages, originally intended only for AP's.

AP1 and AP2 respond by issuing IAPP move response messages 111 and 113 and at that point the access in the AP's is withdrawn for the using entity STA1 in question. Subsequently, the AP's send Dissociate messages 115 and 117 to station STA1 whereby it is possible for an application running on the station, such as a browser, to positively inform the user that access has been withdrawn, as indicated by the lock out indication in step 119.

Hence, according to the invention a network has been provided comprising at least one access point AP1, AP2 and one access controlling node WSN, AS, whereby the identity of the station can be approved by the access controlling node AS. The at least one access-controlling node WSN issues at least one IAPP message causing the AP with which the station is currently associated to disassociate the given station and thereby terminating the access for the given station.

Advantageously, an entity, such as a service provider, could engage an agreement with a given subset of AP's.

According to the invention a method of terminating access for a WLAN station has been provided comprising the steps of

- 5 - monitoring whether a given station is having access to any of a given subset of access points and monitoring an account relating to the given station being associated with a given access point of the subset of access points
- if detecting that the account relating to the given station is zero
- 10 - Issuing an IAPP message causing the access point of the subset with which the given station is associated to disassociate the given station.

According to a second embodiment of the invention, the network topology as in fig. 1 except that no separate WSN node is provided is envisaged. This embodiment is shown
15 in fig. 7. At step 101 it is detected that the account of STA1 is null and the AS issues IAPP move notify messages 121 and 125 over the Internet to AP1 and AP2. The latter AP's take note of what they perceive as a move of STA1 and withdraw access for STA1 to the Internet. Subsequently AP1 and AP2 responds to the AS by issuing IAPP move response messages 123 and 127. Followingly, Disassociate messages 115 and 117 are
20 issued from the AP2 with which the STA1 was recently associated. Disassociate message 117 is received by STA1 whereby the user can be informed as explained above.

In fig. 8 a third embodiment of the invention has been shown wherein a network topology as illustrated in fig. 1 is shown. In this embodiment the WSN or the non-AP network
25 node broadcasts an IAPP ADD-notify frame 129 to all the AP's, which in the case in point amounts to AP1 and AP2. For the AP's it will appear as the STA1 has been associated to a subsequent AP (virtually the WSN) and AP2 with which the STA1 is recently associated will consequently disassociate the UE, by issuing Disassociate messages 115 and 117, the latter being received by STA1.

30

It is noted that since IAPP messages are transported in IP packets, the WSN does not have to reside on the same subnet as the APs. The WSN could send a subnet-directed broadcast to the subnets with the APs of interest. This embodiment has been illustrated
35 in fig. 9.

35

The WSN could also (or instead) broadcast a layer-2 frame with the UE's MAC address as source address to all the APs. This will make all APs believe that the UE has made a handover to a subsequent AP (in this case the subsequent AP is the WSN) and will consequently disassociate the UE.

5

Since, a party not being engaged in providing the actual access for the station in question, is responsible for effectuating the cease of access, one could imagine that denial of service attacks by a rogue AP could be a problem.

10 However, this is not necessarily the case as shall be explained with reference to fig. 10, where a rogue AP, APX, seeks to register as a valid AP, step 80, as described in 802.11F. If, according to known features of RADIUS, the AP cannot show up the necessary credentials, the request will be rejected as exemplified in step 81.

15 Initially when a RADIUS enabled AP client is powered up on the network, step 83, it issues a RADIUS registration access-request 85 to the WSN or the AS, and the latter node responds with a RADIUS registration access-accept containing means for cryptographically protecting IAPP ADD messages.

20 A station STA1 may subsequently associate with an AP, as shown instep 89.

When IAPP messages such as the IAPP ADD notify are received, step 91, 93, 95, the authenticity of these messages as being sent by a proper member of the network can easily be proved by performing a cryptographical operation. If the IAPP message are not
25 cryptographically protected by appropriate keys, the operation will provide a false result and an Denial of Service attack, as illustrated in step 93, will fail, whereas the identity of true RADIUS clients can be ascertained, confer IAPP ADD notify message 95.

30 IEEE 802.11F also provides methods for cryptographically protecting IAPP MOVE messages between two APs. Also these methods utilize a RADIUS server (e.g. WSN or AS) to distribute the key material.

References

- 5 IEEE Standard 802.11-1999; Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
IEEE Standard 802.1X-2001; Port-Based Network Access Control
IEEE Draft Recommended Practice 802.11F
RFC 2865; RADIUS
- 10 RFC 2284: EAP

0307-0311

Claims

1. Network comprising at least one access point (AP1, AP2) and one access controlling node (WSN, AS), the access points making use of the IAPP protocol for inter AP communication, wherein at least one station (STA1) may associate with the access points (AP1, AP2), whereby the identity of the station can be approved by the access controlling node (AS), wherein
 5 the at least one access-controlling node (AS; WSN) issues at least one IAPP message causing the AP with which the station is currently associated to disassociate the given station and thereby terminating access for the given station.
 10
2. Network according to claim 1, wherein a first access-controlling node (AS/ WSN) is an authentication server connected to the Internet.
 15
3. Network according to claim 2, wherein a second access control node is provided, the second access control node being a gateway node (WSN).
 20
4. Network according to claim 2, wherein the access-controlling node issues an IAPP ADD notify message.
 25
5. Network according to claim 2, wherein the access-controlling node issues an IAPP move notify message.
- 30 6. Network according to claim 3, wherein the access-controlling node issues a Lock out request (103) to the gateway node.

10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
180
190
200
210
220
230
240
250
260
270
280
290
300
310
320
330
340
350
360
370
380
390
400
410
420
430
440
450
460
470
480
490
500
510
520
530
540
550
560
570
580
590
600
610
620
630
640
650
660
670
680
690
700
710
720
730
740
750
760
770
780
790
800
810
820
830
840
850
860
870
880
890
900
910
920
930
940
950
960
970
980
990

7. Access controlling node connecting to at least a group of access points, the access points making use of the IAPP protocol for inter AP communication and providing access to at least one station (STA1), the station (STA1), whereby the identity of the station can be approved by the access controlling node (AS), whereby

5

the at least one access-controlling node (AS; WSN) issues at least one IAPP message causing the AP with which the station is currently associated to disassociate the given station and thereby terminating access for the given station.

10

8. Access controlling node according to claim 7, wherein the termination of access is conditional on the exhaustion of an account relating to the given station.

15

9. Method of terminating access for a WLAN station comprising the steps of

monitoring whether a given station is having access to any of a given subset of access points and monitoring an account relating to the given station being associated with a given access point of the subset of access points

20

If detecting that the account relating to the given station is zero

issuing an IAPP message causing the access point of the subset with which the given station is associated to disassociate the given station.

25



Abstract

5 A network is provided comprising at least one access point (AP1, AP2) and one access-controlling node (WSN, AS) whereby the identity of the station can be approved by the access controlling node (WSN, AS). The at least one access-controlling node WSN issues at least one IAPP message causing the AP with which the station is currently associated to disassociate the given station thereby terminating the access for the given station.

10

fig. 6

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194

1/8

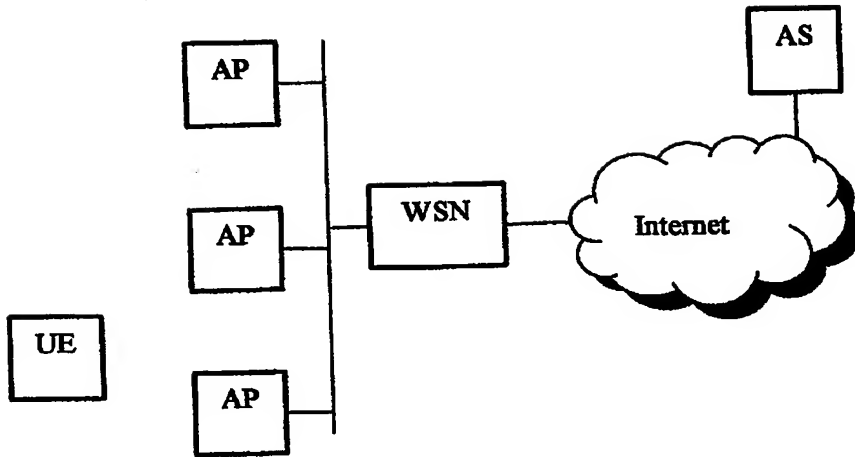


Fig. 1

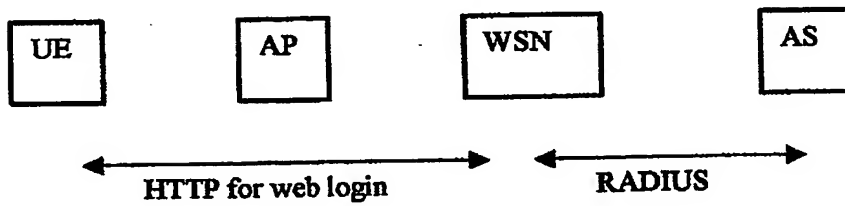


Fig. 2

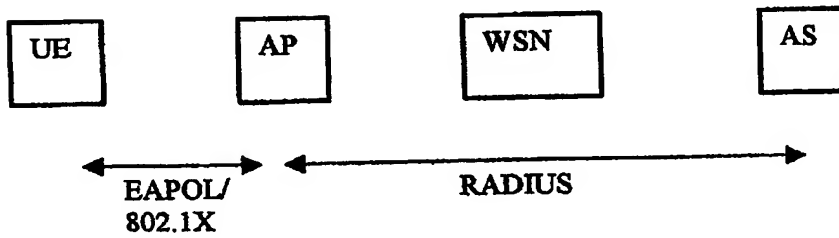


Fig. 3

2/8

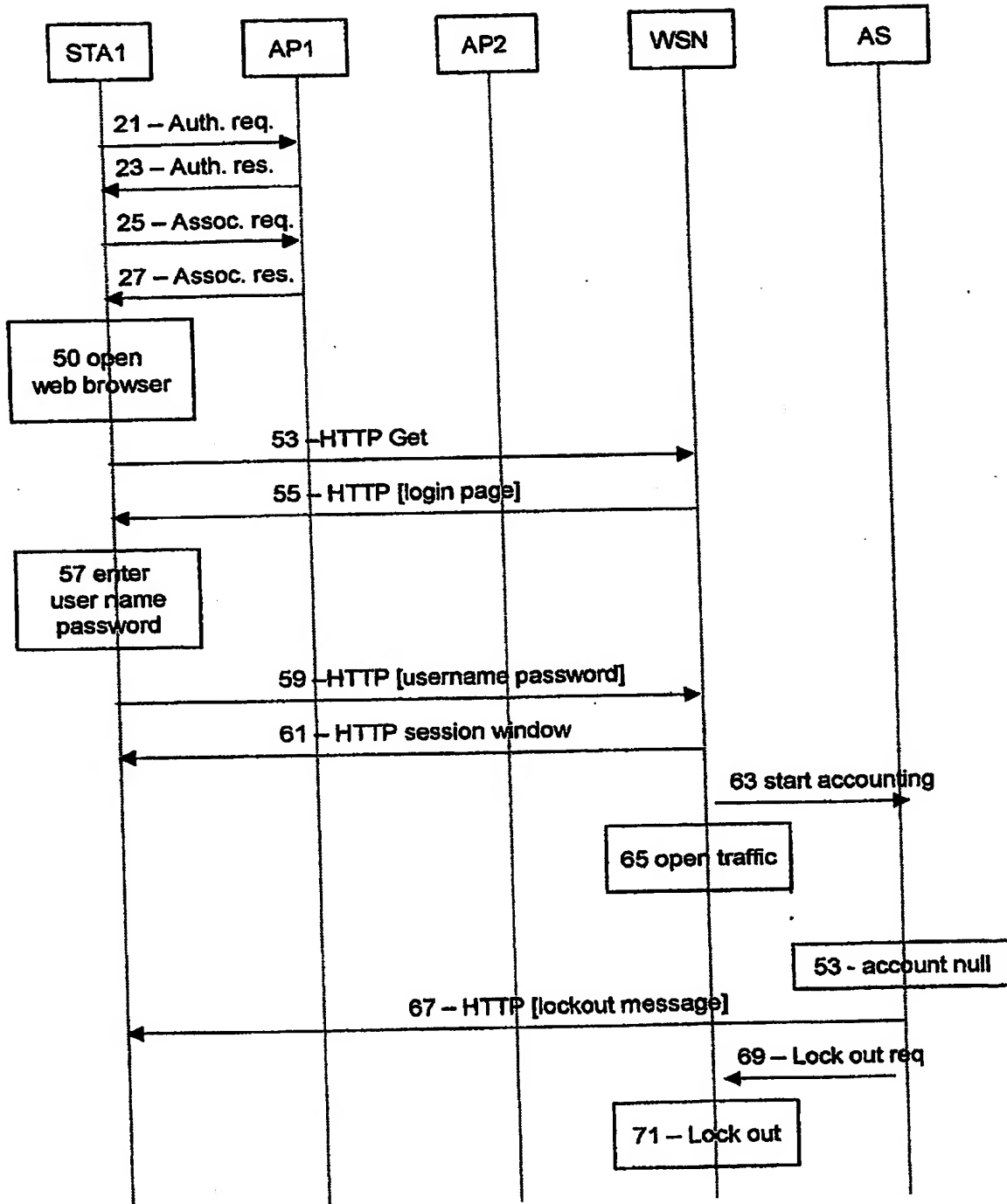


Fig. 4 - prior art

3/8

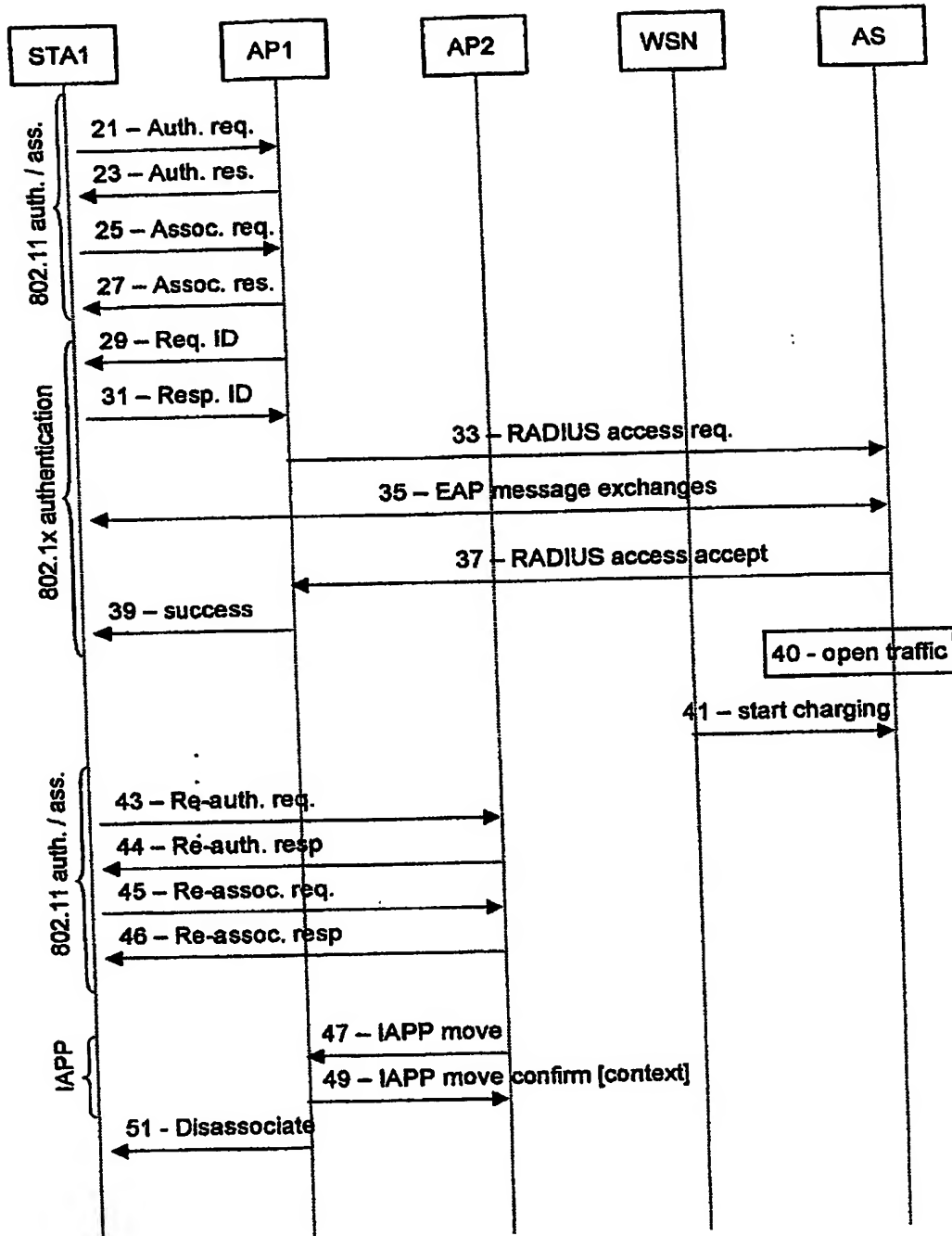


Fig. 5 - prior art

4/8

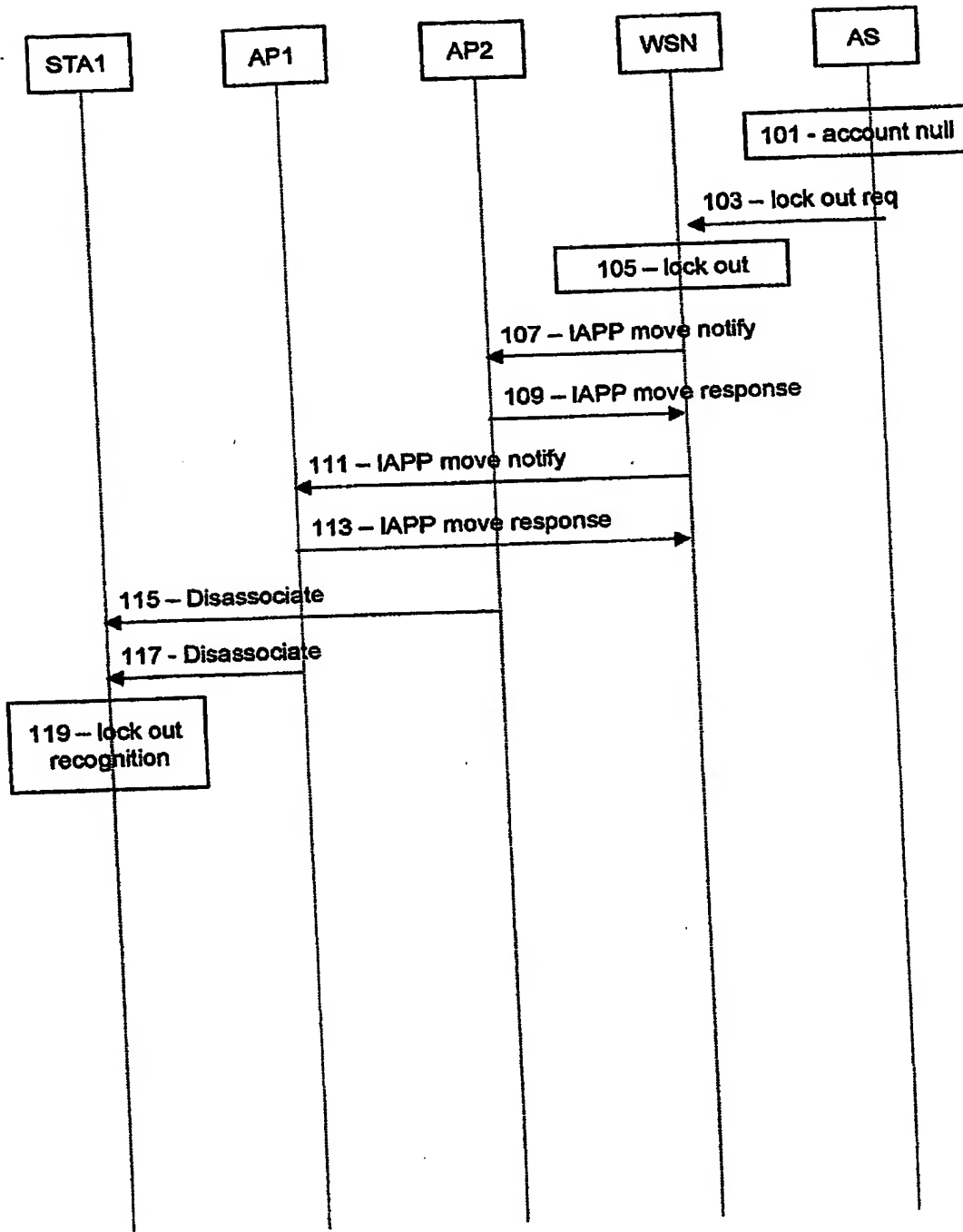


Fig. 6

5/8

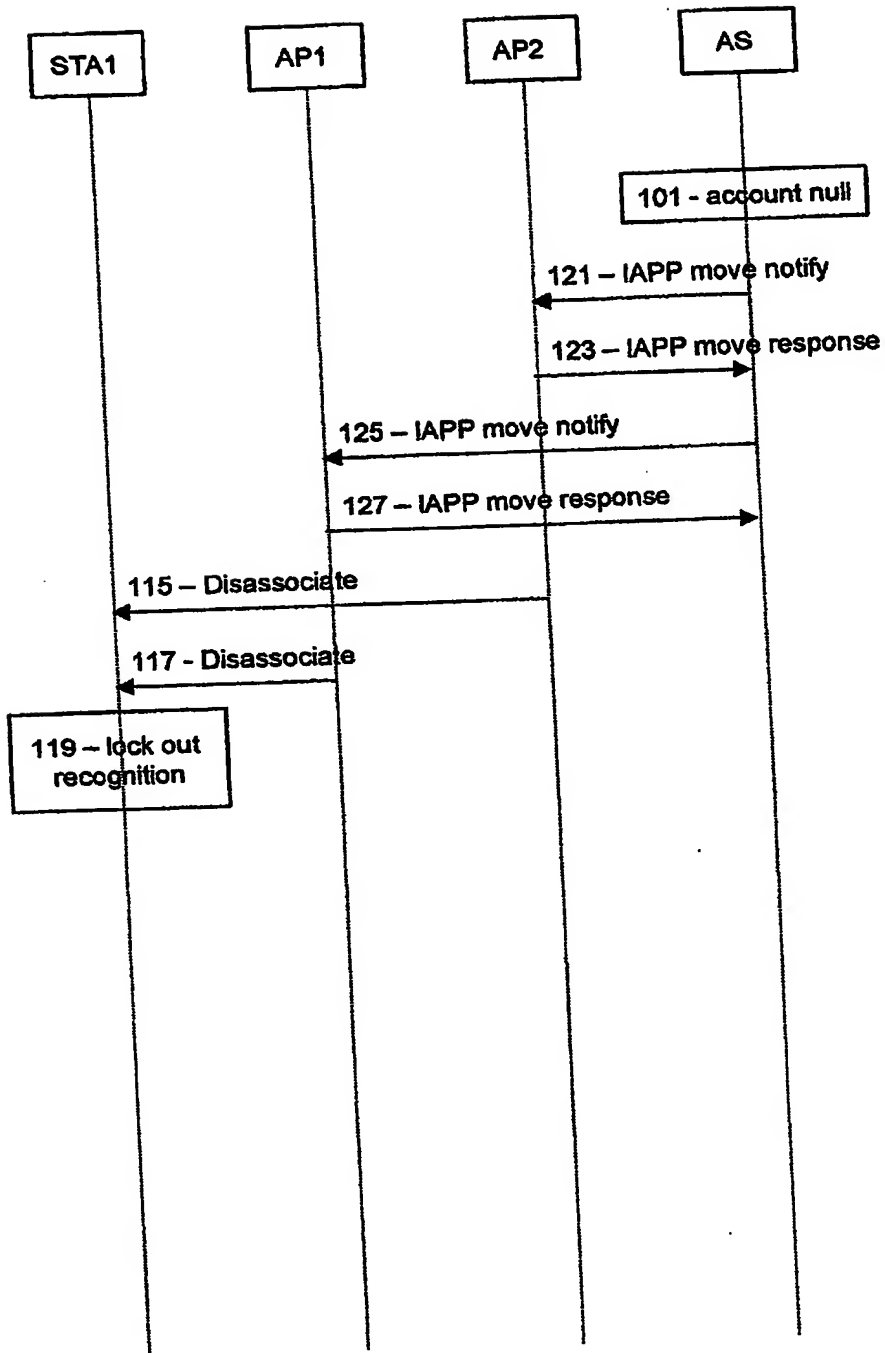


Fig. 7

PRV 03-07-02 H

6/8

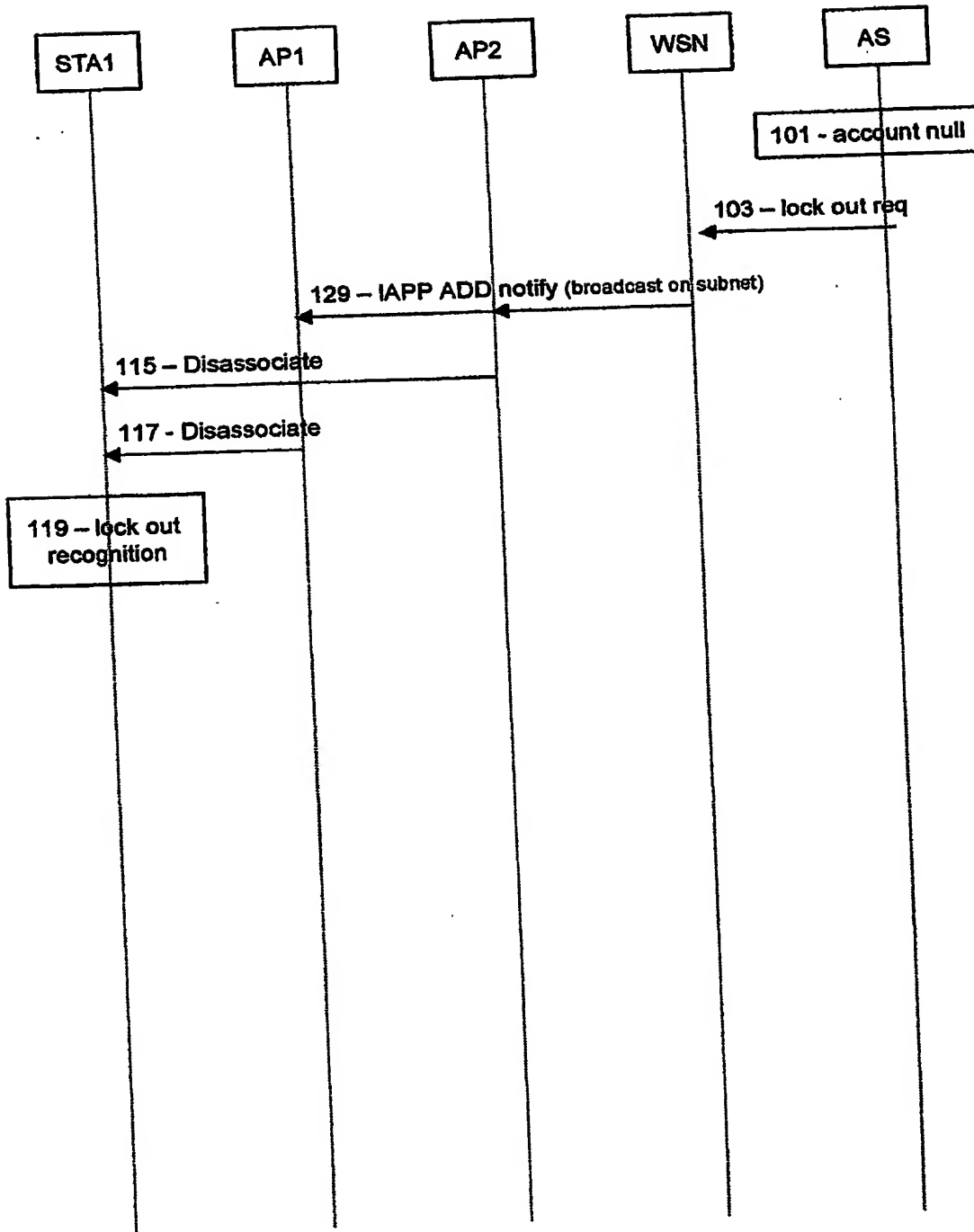


Fig. 8

2003-07-03

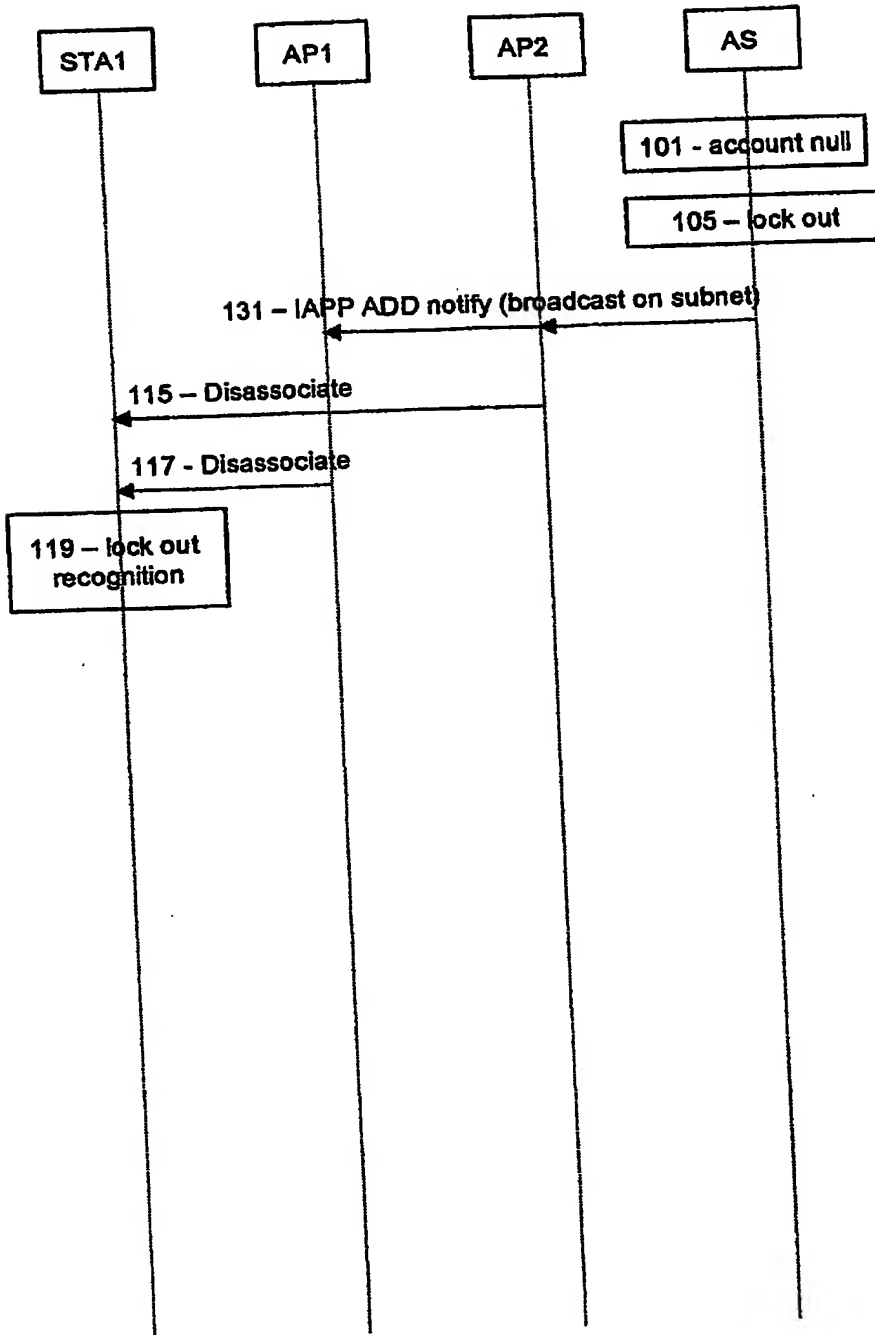


Fig. 9

8/8

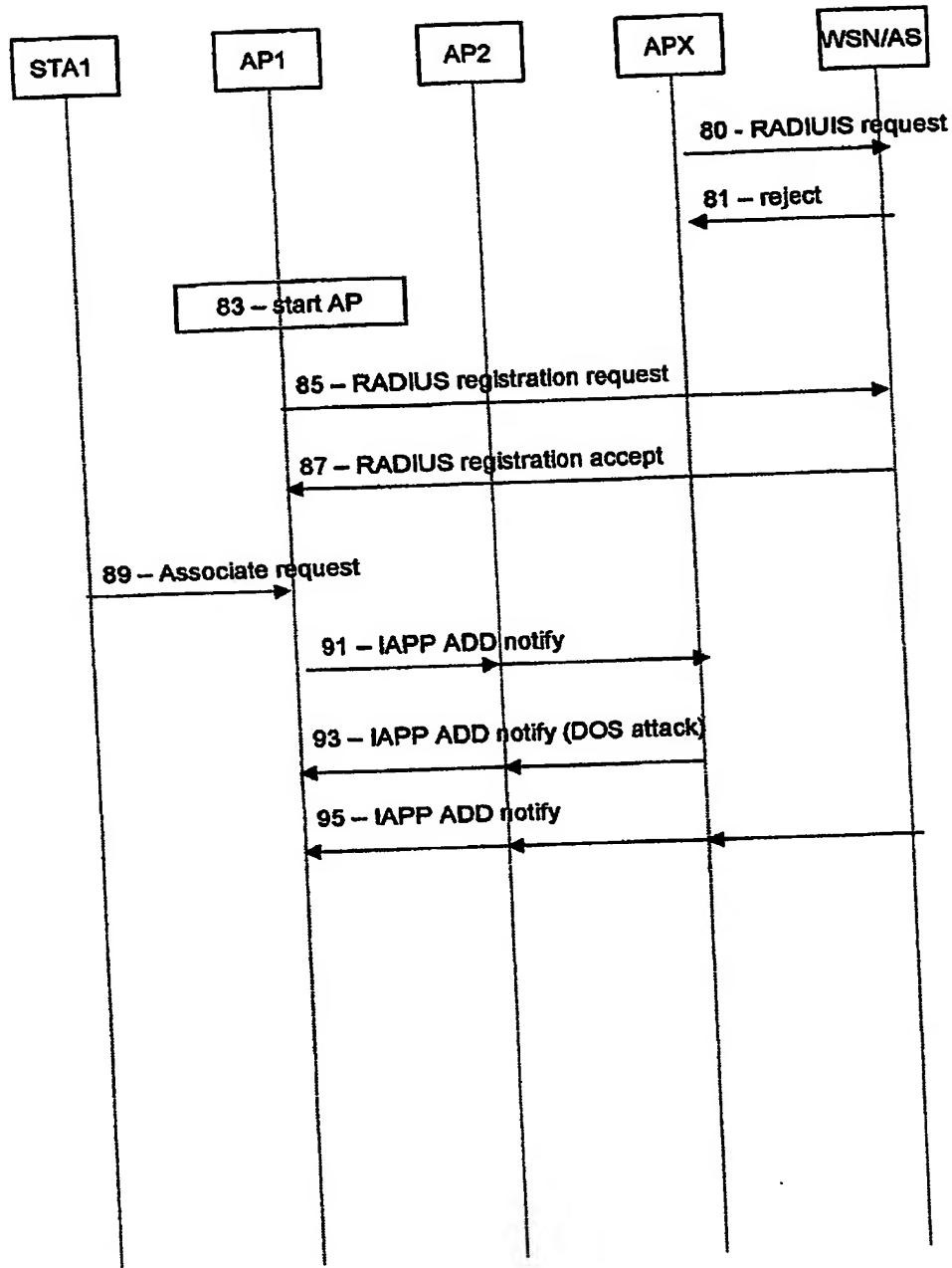


Fig. 10

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ BLACK BORDERS

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☒ FADED TEXT OR DRAWING

☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☐ GRAY SCALE DOCUMENTS

☒ LINES OR MARKS ON ORIGINAL DOCUMENT

☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.